GREGORY (JAS. F.)

[CONFIDENTIAL.]

LETTER

OF

JAMES F. GREGORY,

LIEUT. COLONEL AND A. D. C.,

TO

LIEUT. GENERAL P. H. SHERIDAN,

CONCERNING

TELEGRAPHIC CODE.

WASHINGTON:
GOVERNMENT PRINTING OFFICE.
1886.

[CONFIDENTIAL.]

LETTER

OF

JAMES F. GREGORY,

LIEUT. COLONEL AND A. D. C.,

TO

LIEUT. GENERAL P. H. SHERIDAN,

CONCERNING

TELEGRAPHIC CODE.

WASHINGTON:
GOVERNMENT PRINTING OFFICE.
1886.

[Confidential.]

HEADQUARTERS ARMY OF THE
UNITED STATES,
Washington, D. C., June 11, 1885.

Lieut. Gen. P. H. SHERIDAN,
Commanding Army of the U. S.,
Washington, D. C.

GENERAL: I have the honor to transmit herewith the revised compilation of "Slater's Telegraphic Code," prepared by your direction for the use of the War Department.

In the introduction is given Slater's description of some of the ways in which the code may be used, which is sufficient for publication with the vocabulary. It seems proper to add here, and not for publication with the work, something more about the code and its uses, which may be separately printed if deemed advisable for transmission to those entitled to its use.

In deciding upon this system as best of all those I have examined, where ease of enciphering and deciphering messages, coupled with security from interpretation by persons unacquainted with the key, are the required conditions, I have been strengthened in my opinion of its merits by that of Prof. E. S. Holden, director of the Washburne Observatory, who is an acknowledged expert

Cryptographer. On page 424 of his pamphlet, "The Cipher Dispatches," he says: "The question is often asked, "Is there no safe cipher?" The answer is: there are many such, if one means by a safe cipher one which is almost or quite impossible to translate. The question should be modified so as to include convenience of use, and then the "safe ciphers" are few in number. Perhaps the best and safest cipher for general use is found in Slater's Telegraphic Dictionary of twenty-five thousand words. In this each word is numbered from 00001 to 25,000 consecutively. Suppose the message to be sent was *Rely upon plain English.* The words Rely upon, &c., would be looked out in the dictionary, and the numbers opposite them set down. To these numbers the sender adds a previously agreed upon number, as 4,397, 21,171, &c. He thus obtains four new numbers. These *numbers* are looked out in the dictionary, and the words standing opposite to them are sent. The process of reading the telegram by the receiver of the message is simple. It is not likely that messages of this kind can ever be read by one not acquainted with the key, if this key is occasionally changed, say at the 7th, 10th, 16th, 21st, &c., words. If it is not so changed and there are enough messages, even this code can be read.

Professor Holden, in a letter to me on the subject, has made the following suggestions concerning the uses of the code in correspondence:

1. For messages which are not *very* secret, but yet private, let us take a plan like this: Date message in plain English. For all messages sent

in *January* add 111 to the word number in vocabulary, thus:

Return	19374+111=19485	Rickety
to	22501+111=22612	transaction
Washington.	24789+111=24900	Spokane (Ft.)

The message sent would be: Rickety transaction, Spokane (Ft.).

For all messages in *February* add 222, in *March* 333, &c.

This key could be known to many people and yet be safe enough. Next year make *January* some other number or change at any time.

A simple complication of this is to add 111 for January and also to add (or subtract) as many units as make the day of the month; thus for *January* 20, add 111 + 20 = 131; you have then 365 keys per year, and all simple.

A simple message in ordinary English: "Add 1437 to all ciphers until further orders," would complicate this (for the decipherer) and yet leave it all clear for those possessing the key.

Whatever scheme be used be careful to have it easy, for it is very hard to decipher the very easiest one of this kind, and a simple one only is needed for general private correspondence.

2d. For more private messages, but which it is desirable not to make too complicated.

An arbitrary code like the following might do for these: Add to the 1, 2, 3, 4, ...nth word of message 15, 25, 35, 45 . ... (n+5) or in general (10+a) (20+a) (30+a).....(n+a).

This is perfectly simple in use and absolutely impossible to decipher if it is changed occasion-

ally—that is, if *a* is made a′, a″, &c., once a month or even a year.

3d. For the few messages which need be carefully guarded and kept secret from all but a very few, the preceding plan might be used, modified by reversing 1, 2, 3, 4, of the digits either of the *message* proper, or of (n+a). There are endless simple ways of doing this, but it should always be remembered the deciphering of the easiest of these ciphers is *very* hard—to the man without the key.

To denote to the recipient of a message which scheme is used, certain signs may be employed, such as placing date at beginning or end of a message, by inserting arbitrary numbers in a message, or what not.

One of the many complications easy to use is this: Write the message and *change* the *code* at every, or every other, or every tenth, or every hundredth word, thus:

Achievable	301	19675 rotundity.
Return	19374	
Addict	401	22902 unbiased.
To	22501	
Ado	501	25290 accuse.
Washington	24789	

The message is: Achievable, rotundity addict unbiased ado accuse.

The above illustrations are deemed ample for a thorough understanding of the uses that may be made of the book. The special schemes to be devised for practical use should be privately made known to those entitled to use them by letter or by word of mouth.

The labor of compiling the vocabulary has been performed by Mr. W. G. Spottswood.

I have the honor to request that when printed the proof-sheets of this work be submitted to me for revision. The size of page most convenient for use is six and a half inches by four inches.

Very respectfully, your obedient servant,

JAMES F. GREGORY,

Lieut. Colonel and A. D. C.